



AF

IFW

Practitioner's Docket No.: 070051-0290630  
Client Reference No.: 110072601/JEB/UBR

**PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of:

Confirmation No: 1088

ÖSTBERG ET AL.

Application No.: 10/050,065

Group No.: 2142

Filed: January 15, 2002

Examiner: M. MEUCCI

For: SECURE TOP DOMAIN

**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, VA 22313-1450**

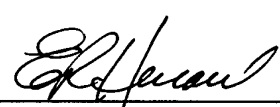
**SUBMISSION OF PRIORITY DOCUMENT**

Attached please find the certified copy of the foreign application from which priority is claimed for this case:

<u>Country</u>	<u>Application Number</u>	<u>Filing Date</u>
Sweden	0104364-5	December 21, 2001

Date: May 1, 2007

PILLSBURY WINTHROP SHAW PITTMAN LLP  
P.O. Box 10500  
McLean, VA 22102  
Telephone: (703) 770-7900  
Facsimile: (703) 770-7901  
Customer Number: 00909

  
\_\_\_\_\_  
E. Rico Hernandez  
Reg. No. 47641

# PRV

PATENT- OCH REGISTRERINGSVERKET



## Intyg Certificate

Härmed intygas att bifogade kopior överensstämmer med de handlingar som ursprungligen ingivits till Patent- och registreringsverket i nedannämnda ansökan.

This is to certify that the annexed is a true copy of the documents as originally filed with the Patent- and Registration Office in a connection with the following patent application.

- (71) Sökande: Altrax AB, Malmö, SE  
Applicant (s)
- (21) Patentansökningsnummer 0104364-5  
Patent application number
- (86) Ingivningsdatum 2001-12-21  
Date of filing

Stockholm, 2007-04-02

För Patent- och registreringsverket  
For the Patent- and Registration Office

William Ddumba

Avgift

Fee 170:-

## **Tekniskt område**

Föreliggande uppfinning hänför sig till en spärranordning för oönskad nättrafik i öppna dator- och telekommunikationsnätverk såsom Internet, och ett förfarande för det samma.

5

## **Teknikens ståndpunkt**

Internet ses av många som en ostrukturerad marknadsplats där det saknas en helhetsbild. Härvid existerar det oönskade sajter i form av enl lagen förbjuden pornografi, terrorism, ekonomisk brottslighet mm. Ett annat problem utgörs av hackers och datorviruspridare. Med andra ord upplevs t ex Internet sakna en önskad struktur för seriösare eller sanerad nättrafik.

Nuvarande toppdomäner såsom .com, .arpa, .edu, .net med flera ställer få krav eller inga på sajter avseende goda seder och bruk (ordre public).

Hemsidor är dyra att etablera och att underhålla, vilket medför att tjänster över Internet blir kostsamma. Detta fenomen har nyligen upplevts av branschen, speciellt beträffande säljsajter på Internet, vilka i många fall har gått i konkurs. Försök görs att erhålla direkta intäkter för gjorda investeringar genom t ex banners, pop-ups, medlemskap, lösenord mm.

Sammantaget finns det ett stort behov av en tillförlitlig struktur över www och liknande så att användare och tjänsteleverantörer kan känna trygghet i användandet av www vad avser sånt som strider mot goda seder och bruk samt hur en avkastning för en ordnad struktur skall genereras.

## **Sammanfattning av den beskrivna uppfinningen**

Föreliggande uppfinning avser att ange en lösning till problemet med oönskad nättrafik i öppna dator- och telekommunikationsnätverk, speciellt på world wide web (www) via Internet eller liknande.

För att åstadkomma en lösning på nämnda problem anger föreliggande uppfinning en spärranordning för oönskad nättrafik i öppna dator- och Telekommunikationsnätverk. Anordningen innefattar härvid:

en första spärrnivå i form av en toppdomän som kräver registrering för web-sajter under domänen avseende ordre public;

åtminstone en toppdomänserver för anslutning mot toppdomänen innefattande eller ansluten mot domännamnserver -filer och -programvara, vilka tilldelar ett anrop genom dator en nätverksadress som associerar till rätt tillämpningsserver, när datorns användare har identifierats;

databasorgan, anslutna mot toppdomänservern, för registrering och godkännande av en tjänsteförmedlare under toppdomänen;

organ anslutna mot eller innefattade i toppdomänservern för identifiering av en anropandes identitet vid uppkoppling mot toppdomänen;

5 organ anslutna mot eller innefattade i toppdomänservern för spärrning av en oidentifierad anropande; och

varvid registreringen av anslutna mot domänen och identifieringen av en anropande förhindrar fri anslutning resp anonymitet i datornätverk via nämnda toppdomänserver, vilket åstadkommer en toppdomän som är sanerad från oönskad nättrafik.

10 I en utföringsform av uppfinningen åstadkommes en andra spärrnivå, som innefattar mikrodebitering via en debiteringsserver vid anslutning mot toppdomänen, varvid följande organ innefattas:

organ för debitering av toppdomänen via mikrodebiteringen;

15 organ för ackumulering av nämnda mikrobetalning för varje session som en användare är uppkopplad mot nämnda domän.

En annan utföringsform åstadkommer att den uppkopplandes web-adress lagras för debitering i databasen.

Ytterligare en utföringsform åstadkommer organ, via debiteringsservern, för procentuell uppdelning i åtminstone två poster ackumulerade mikrodebiteringar för varje session under uppkopplingen, vilka poster krediteras åtminstone en av toppdomänen och en registrerad tjänsteleverantör.

Föreliggande uppfinning anger även ett förfarande avseende en spärranordning för oönskad nättrafik i öppna dator-och telekommunikationsnätverk. Härvid innefattar förfarandet följande steg:

25 anordnande av en första spärrnivå i form av en toppdomän som kräver registrering för web-sajter under domänen avseende ordre public;

anslutning av åtminstone en toppdomänserver mot toppdomänen innefattande eller ansluten mot domännamnserver -filer och -programvara, vilka tilldelar ett anrop genom dator en nätverksadress som associerar till rätt tillämpningsserver, när datorns användare har identifierats;

30 anslutning av databasorgan mot toppdomänservern, för registrering och godkännande av en tjänsteförmedlare under toppdomänen;

identifiering av en anropandes identitet vid uppkoppling mot toppdomänen via organ för detsamma;

spärning via organ för detsamma av en oidentifierad anropande; och  
varvid registreringen av anslutna mot domänen och identifieringen av en  
anropande förhindrar fri anslutning resp anonymitet i datornätverk via nämnda  
toppdomänserver, vilket åstadkommer en toppdomän som är sanerad från oönskad nättrafik.

5 I en utföringsform av förfarandet enligt föreliggande uppfinning anges att en  
andra spärrnivå innefattar mikrodebitering via en debiteringsserver vid anslutning mot  
toppdomänen via:

organ för debitering av toppdomänen via mikrodebiteringen;  
organ för ackumulering av nämnda mikrobetalning för varje session som en  
10 användare är uppkopplad mot nämnda domän.

Förfarandet enligt föreliggande uppfinning kan även utöva andra  
utföringsformer för spärranordningen enl ovan.

#### Kortfattad beskrivning av ritningar

Fortsättningsvis hänvisas fortlöpande i beskrivningstexten till bilagda  
15 ritningsfigurer för en bättre förståelse av exemplifieringar och utföringsformer av  
föreliggande uppfinning, varvid:

**Fig. 1** schematiskt illustrerar en första spärrnivå för spärranordningen enligt  
föreliggande uppfinning på blockschema form i ett öppet nätverk för data- och  
telekommunikation;

20 **Fig. 2** illustrerar schematiskt en andra spärrnivå i spärranordningen enligt fig. 1;  
och

**Fig. 3** illustrerar hur en användare slussas mot en toppdomän enligt föreliggande  
uppfinning.

#### Detaljerad beskrivning av föredragna utföringsformer

25 För att lösa problem med oönskad web-baserad trafik och sanera denna från t ex  
barnpornografi, hackers, virusspidare, ekonomisk kriminalitet mm, anger föreliggande  
uppfinning en ny toppdomän (Top Level Domain, TLD). En ny TLD är i sig inget  
märkvärdigt, men om den förknippas med villkor för dess användande via därför avsedda  
organ kan den enligt föreliggande uppfinning lösa de problem som tidigare nämnts.

30 I fig. 1 illustreras schematiskt spärranordningen enligt föreliggande uppfinning  
på blockschema form i ett öppet nätverk för data- och telekommunikation. Uppfinningen  
anger två spärrnivåer för oönskad trafik på ett nätverk såsom Internet eller liknande, varvid  
nivåerna är:

1. Spärning via registrering av web-sajter under toppdomänen, varvid registrerade web-sajter godkänns efter granskning under satta kriterier för den nya TLDn.
2. Uppkoppling mot TLDn genererar mikrobetalningar.

5

I föreliggande beskrivning är nivå 2 en utföringsform utav nivå 1. Fig. 1 illustrerar nivå 1 förr spärning av ej önskade websajter där dubbelriktade pilar anger kommunikationsvägar över www 10. Fig. 1 visar www 10 såsom Internet, en dator 12 ansluten mot www 10, en domännamnsserver 14 (Domain Name Server, DNS), TLD-server 16, en databas 18 för registrering av godkända web-sajter under toppdomänen och en tjänsteförmedlare 19 över Internet (Internet Service Provider). Tjänsteleverantörer 19 över Internet måste således godkännas för registrering i TLD-server 16 databas 18 innan tjänster får förmedlas under toppdomänen enl föreliggande uppfinning. Detta utgör en nivå 1 spärning under toppdomänen korrelerat med att inga TCP/IP adresser från användare med dator 12 som inte går att identifiera släpps fram i domänen, utan spärras tillträde och ev registrering i databasen 18. TLD-servern 16 innefattar i en utföringsform organ för att ställa frågor mot ansluten dator 12 för att identifiera denna och dess användare.

En DNS 14 innehåller program och filer som bildar en DNS-databas där en nätadress t ex xxx@yy.net omvandlas till en IP-adress som associerar till rätt tillämpningsserver.

För att åstadkomma spärning för oönskad web-trafik anger föreliggande uppfinning en spärranordning för oönskad nättrafik i öppna dator- och telekommunikationsnätverk. Den innefattar en första spärrnivå i form av en toppdomän som kräver registrering för web-sajter under domänen avseende ordre public. Vidare innefattar den åtminstone en toppdomänserver 16 för anslutning mot toppdomänen, innefattande eller ansluten mot domännamnsserver 14 -filer och -programvara, vilka tilldelar ett anrop/uppkoppling genom dator 12 en nätverksadress som associerar till rätt tillämpningsserver, när datorns 12 användare har identifierats. Det finns databasorgan 18, som är anslutna mot toppdomänservern 16, för registrering och godkännande av en tjänsteförmedlare 19 under toppdomänen.

Ytterligare innefattas organ anslutna mot eller innefattade i toppdomänservern 16 för identifiering av en anropandes identitet vid uppkoppling mot toppdomänen, och organ anslutna mot eller innefattade i toppdomänservern 16 för spärning av en oidentifierad anropande. Registrering av anslutna mot domänen och identifieringen av en anropande

förhindrar fri anslutning resp anonymitet i datornätverk genom toppdomänservern 16, vilket åstadkommer en toppdomän som är sanerad från oönskad nättrafik.

DNS-programvara 14 och filer som innefattas eller är anslutna mot toppdomänservern 16 kan direkt användas för att alstra IP-adresser till sajter för giltiga och identifierbara användare/uppkopplare mot toppdomänen.

I enlighet med fig. 2 illustreras schematiskt en andra säkerhetsnivå för att spärra oönskad nättrafik över den förutbestämda toppdomänen. I figuren har det tillkommit en debiteringsserver 20 (billing server) för mikrobetalningar vid uppkoppling mot toppdomänen, dvs alla användare med datorer 12 kommer att debiteras så fort de är uppkopplade mot domänen. Detta förhindrar opåkallad nät-surfning.

Den andra spärrnivån innefattar mikrodebitering vid anslutning mot toppdomänen genom organ för debitering av toppdomänen via mikrodebiteringen samt organ för ackumulering av mikrobetalningar för varje session som en användare är uppkopplad mot domänen. För mikrobetalningar finns en rad på marknaden kända förfaranden, t ex sändning av tidsbaserade ticks. En uppkopplandes web-adress kan då lagras för debitering i databasen 18 och/eller annan databas relaterad till debiteringsservern 20.

Betalningsmottagare för mikrodebiteringarna är företrädesvis tjänsteleverantören 19 och en administratör av den nya toppdomänen via organ för procentuell uppdelning i åtminstone två poster ackumulerade mikrodebiteringar för varje session under uppkopplingen.

Fig. 3 illustrerar schematiskt ett flödesschema av en utföringsform för föreliggande uppfinning. En användare/uppkopplare med dator 12 loggar in 300 mot toppdomänen, varvid organen för spärr kontrollerar 310 om uppkopplarens adress och/eller en användare är känd, vilket villkoras 320. Om adressen och/eller användaren inte är identifierbar sker ingen anslutning 330 mot toppdomänen.

I fall av att anslutning mot toppdomänen åstadkommes enligt spärrnivå 1 och villkoret 320 är ja då tilldelar DNS 14, eller liknande programvara, den adressat som uppkopplaren vill nå, t ex www.zzz.net en IP-adresskod 340. Vid tilldelning av IP-adresskoden passeras spärrnivå 1, 350, varvid den sökta sajten 390, via ISP 380 i toppdomänen, ansluts mot datorn 12 samtidigt som nivå 1 spärren har passerats 380.

Om anslutningen åstadkommes enligt spärrnivå 2 villkoras 360 om debitering skall ske eller inte. Villkoraren 360 är fysiskt sett en omkopplare, som en administratör av spärranordningen enligt föreliggande uppfinning råder över, varvid den exempelvis kan kopplas in och ur beroende på om vissa tider skall vara debiteringsfria. Vid ja-villkor uppnås

nivå 2 spärr 400 och både nivå 1 och nivå 2 spärr gäller. Nivå 2 spärr passage triggar 410 nu en mikrodebitering mot användaren, vilken ackumuleras i t ex debiteringsservern 20. Då debitering inte accepteras sker ingen anslutning mot toppdomänen 330. Efter det att servern 20 har anslutits kan uppkoppling via dator 12 nu åstadkommas mot toppdomänen 370 och  
5 anslutning mot exempelvis en ISP och vidare mot sökt sajt 390.

I föreliggande beskrivning nämnda organ består företrädesvis av inom teknikområdet förut känd mjukvara, hårdvara eller av en kombination av båda.

Även om föreliggande uppfinning har beskrivits genom specifika exempel och utföringsformer anger bilagda patentkravs avfattning ytterligare utföringsformer för en  
10 fackman inom teknikområdet.

-----

PR01-1221



**Patentkrav**

1. Spärranordning för oönskad nättrafik i öppna dator- och telekommunikationsnätverk (10), **k ä n n e t e c k n a d** av att den innefattar:

5 en första spärrnivå (350) i form av en toppdomän som kräver registrering för web-sajter (390) under domänen avseende ordre public;

åtminstone en toppdomänserver (16) för anslutning mot toppdomänen innefattande eller ansluten mot domännamnserver (14) -filer och -programvara, vilka tilldelar ett anrop genom dator (12) en nätverksadress (340) som associerar till en rätt  
10 tillämpningsserver (380) när datorns (12) användare har identifierats;

databasorgan (18), anslutna mot toppdomänservern (16), för registrering och godkännande av en tjänsteförmedlare (19) under toppdomänen;

organ anslutna mot eller innefattade i toppdomänservern (16) för identifiering av en anropandes identitet (310) vid uppkoppling mot toppdomänen;

15 organ anslutna mot eller innefattade i toppdomänservern (16) för spärrning (330) av en oidentifierad anropande; och

varvid registreringen av anslutna mot domänen och identifieringen av en anropande förhindrar fri anslutning resp anonymitet i datornätverk via nämnda toppdomänserver (16), vilket åstadkommer en toppdomän som är sanerad från oönskad  
20 nättrafik.

2. Spärranordning enligt krav 1, **k ä n n e t e c k n a d** av att en andra spärrnivå (400) innefattar mikrobeitering via en debiteringsserver (20) vid anslutning (410) mot toppdomänen via:

organ för debitering av toppdomänen via mikrobeiteringen;

25 organ för ackumulering av nämnda mikrobetalning för varje session som en användare är uppkopplad mot nämnda domän.

3. Spärranordning enligt krav 2, **k ä n n e t e c k n a d** av att den uppkopplandes (12) web-adress lagras för debitering i en databas (18).

4. Spärranordning enligt krav 3 eller 2, **k ä n n e t e c k n a d** av att den  
30 innefattar:

organ i debiteringsservern (20) för procentuell uppdelning i åtminstone två poster ackumulerade mikrobeiteringar för varje session under uppkopplingen, vilka poster krediteras åtminstone en av toppdomänen och en registrerad tjänsteleverantör.

5. Förfarande avseende en spärranordning för oönskad nättrafik i öppna dator- och telekommunikationsnätverk (10), **k ä n n e t e c k n a t** av att de innefattar förfarande stegen:

- anordnande av en första spärrnivå (350) i form av en toppdomän som kräver registrering för web-sajter (390) under domänen avseende ordre public;
- anslutning av åtminstone en toppdomänserver (16) mot toppdomänen innefattande eller ansluten mot domännamnserver (14) -filer och -programvara, vilka tilldelar (340) ett anrop genom dator (12) en nätverksadress som associerar till rätt tillämpningsserver (380), när datorns (12) användare har identifierats;
- anslutning av databasorgan (18) mot toppdomänservern (16), för registrering och godkännande av en tjänsteförmedlare (19) under toppdomänen;
- identifiering av en anropandes identitet (320) vid uppkoppling mot toppdomänen via organ för detsamma;
- spärming (330) via organ för detsamma av en oidentifierad anropande; och
- varvid registreringen av anslutna mot domänen och identifieringen av en anropande förhindrar fri anslutning resp anonymitet i datornätverk via nämnda toppdomänserver (16), vilket åstadkommer en toppdomän som är sanerad från oönskad nättrafik.

6. Förfarande avseende en spärranordning enligt krav 5, **k ä n n e t e c k n a t** av att en andra spärrnivå innefattar mikrodebitering via en debiteringsserver (20) vid anslutning mot toppdomänen via:

- organ för debitering av toppdomänen via mikrodebiteringen;
- organ för ackumulering av nämnda mikrobetalning för varje session som en användare är uppkopplad mot nämnda domän.

7. Förfarande avseende en spärranordning enligt krav 6, **k ä n n e t e c k n a t** av att den uppkopplandes web-adress lagras för debitering i en databas (18).

8. Förfarande avseende en spärranordning enligt krav 6 eller 7, **k ä n n e t e c k n a t** av att det i debiteringsservern (20) innefattas organ för procentuell uppdelning i åtminstone två poster ackumulerade mikrodebiteringar för varje session under uppkopplingen, vilka poster krediteras åtminstone en av toppdomänen och en registrerad tjänsteleverantör.

-----

**Sammandrag**

Uppfinningen avser en spärranordning för oönskad nättrafik i öppna dator- och telekommunikationsnätverk (10) och ett förfarande för detsamma. För att åstadkomma spärr för sajter (390) som strider mot ordre public existerar två spärrnivåer (350, 400) genom en  
5 toppdomän med registrering av sajter (390) och mikrodebiteringar.  
(Fig. 3)

-----

PRV01.12.01

1/2

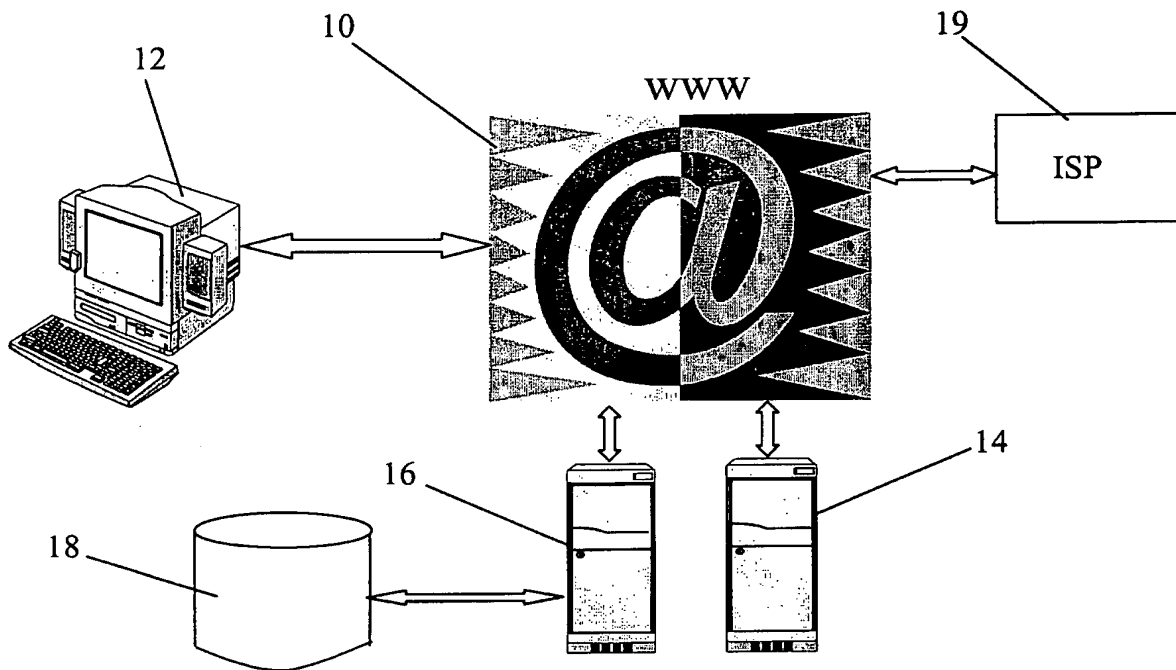


Fig. 1

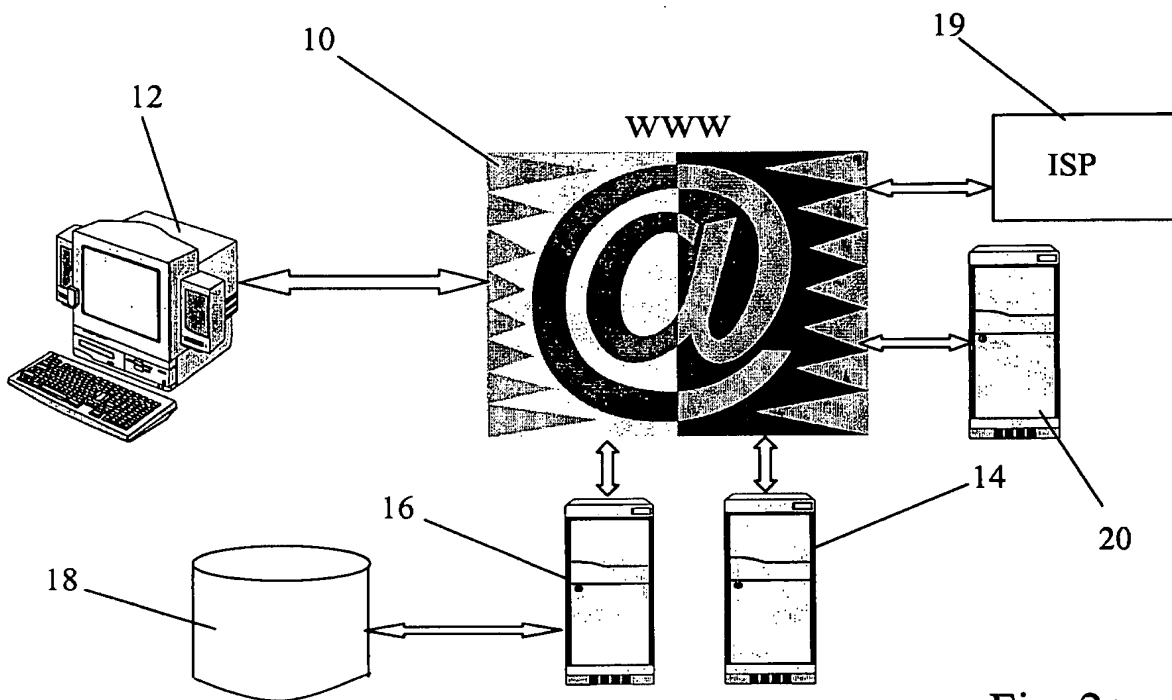


Fig. 2

PRV01.12.21

2/2

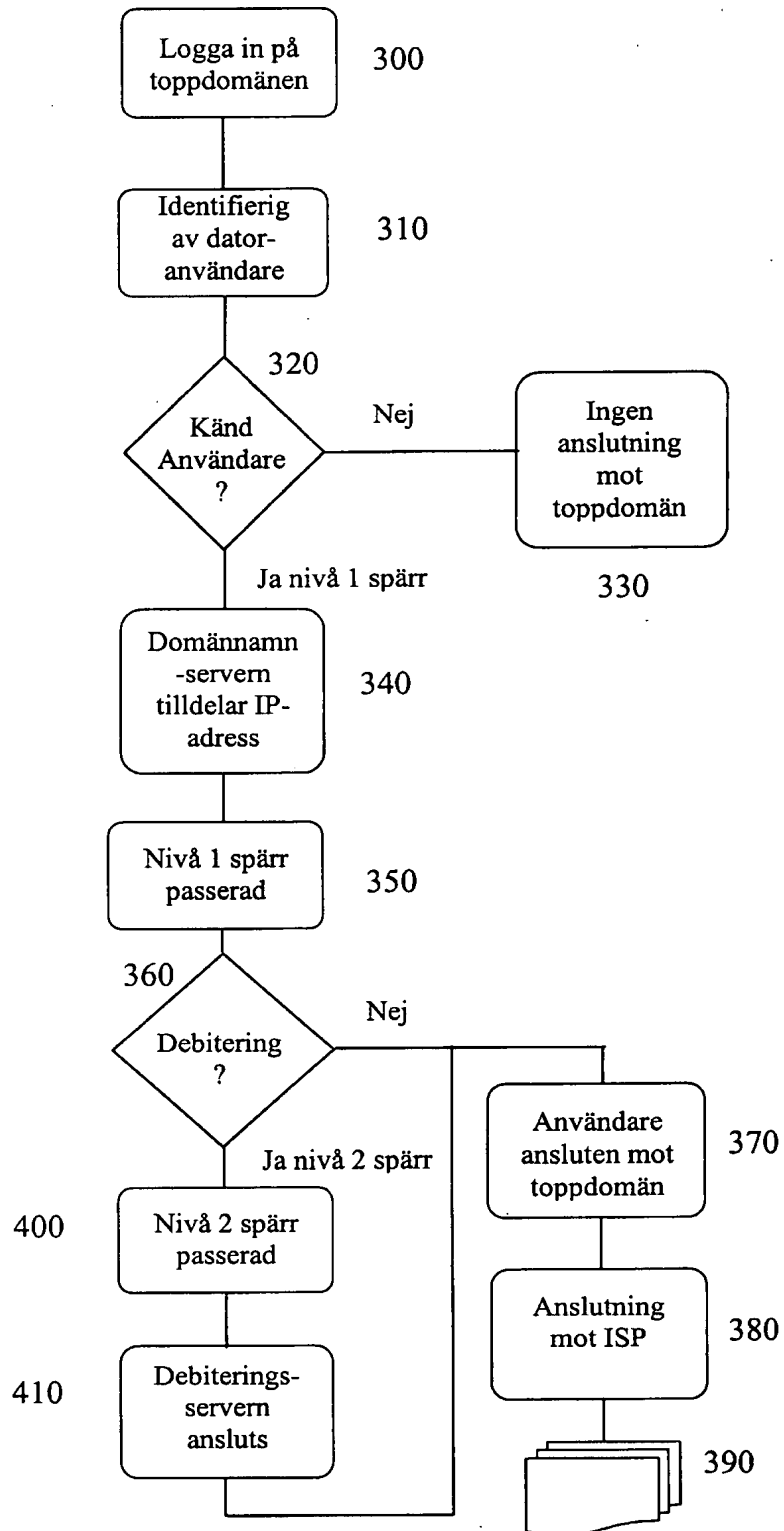


Fig. 3